UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

WHATSAPP INC., et al.,

Plaintiffs,

v.

NSO GROUP TECHNOLOGIES LIMITED, et al.,

Defendants.

Case No. 19-cv-07123-PJH

ORDER RE MOTIONS TO COMPEL AND MOTION FOR RELIEF FROM CASE MANAGEMENT ORDER

Re: Dkt. No. 235, 236, 239, 240, 249, 257, 260, 264, 265, 272, 276, 279, 280

Before the court are plaintiffs' motion to compel discovery, defendants' motion to compel discovery, and defendants' motion for relief from the case management schedule. The motions came on for hearing on February 15, 2024. Plaintiffs WhatsApp Inc. and Facebook, Inc. appeared through their counsel, Antonio Perez-Marques, Craig Cagney, Micah Block, and Greg Andres. Defendants appeared through their counsel, Joseph Akrotirianakis and Aaron Craig. Having read the parties' papers and carefully considered their arguments and the relevant legal authority, and good cause appearing, the court rules as follows.

BACKGROUND

On October 29, 2019, plaintiffs filed this lawsuit, alleging that defendants sent spyware, using WhatsApp's system, to approximately 1,400 mobile phones and devices designed to infect those devices for the purpose of surveilling the users of those phones and devices. Dkt. 1, ¶ 1. The complaint alleges four causes of action: (1) violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030; (2) violation of the California

Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502; (3) breach of contract; and (4) trespass to chattels.[1]

Defendants previously filed a motion for protective order, seeking an order excusing it from compliance with discovery obligations due to various U.S. and Israeli restrictions. See Dkt. 186. The court denied defendants' motion to the extent that it sought a blanket order excusing it from all discovery, but also concluded that defendants may be partially excused from certain discovery obligations based on the framework set forth by Richmark Corp. v. Timber Falling Consultants, 959 F.2d 1468, 1475 (9th Cir. 1992). See Dkt. 233.

The Richmark court set forth the following factors for a court to consider "in deciding whether or not foreign statutes excuse non-compliance with discovery orders:" (1) the importance to the investigation or litigation of the documents or other information requested, (2) the degree of specificity of the request, (3) whether the information originated in the United States, (4) the availability of alternative means of securing the information, (5) and the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interests of the state where the information is located. 959 F.2d at 1475.

After considering Richmark as applied to this case, the court concluded that "to the extent that discovery disputes arise between the parties, the court's analysis will focus on factors (1) and (2), and in instances where the requested discovery is sufficiently important and specific, the court will order compliance with those discovery requests." Dkt. 233 at 10.

Plaintiffs' motion to compel discovery now raises a dispute where the discovery requests must be analyzed as to factor (1) and (2), i.e., the importance of the requests to the litigation, and the degree of specificity of the requests.

[1] The court dismissed plaintiffs' fourth cause of action under Rule 12(b)(6), and no amended complaint was filed. See Dkt. 111. That leaves only the first three causes of action as operative claims in this case.

Defendants have also filed a motion to compel discovery that does not relate to the Richmark factors, as well as a motion for relief from the case management schedule. Those motions will be addressed after addressing plaintiffs' discovery motion. The parties have also filed a number of motions to seal (Dkt. 235, 239, 249, 257, 260, 264, 272, 276), which are GRANTED.

DISCUSSION

A. Plaintiffs' motion to compel discovery (Dkt. 236)

As an initial matter, as stated at the hearing, defendants have already conceded that some of plaintiffs' requests do seek information that is sufficiently important and specific under Richmark, and those documents must indeed be produced. See Dkt. 252 at 5. As to the remaining discovery sought by plaintiffs' motion, the court will address those requests with reference to the four categories set forth in the parties' briefs: (1) what versions of the alleged spyware must be produced, (2) what functionality of the alleged spyware must be produced, (3) whether defendants' clients must be disclosed, and (4) whether defendants' server architecture information must be disclosed. See Dkt. 236 at 12.

As to category (1), as stated at the hearing, the court adopts plaintiffs' definition of "all relevant spyware" as set forth in their motion: "any NSO spyware targeting or directed at Whatsapp servers, or using Whatsapp in any way to access Target Devices." See Dkt. 236 at 13. As also stated at the hearing, defendants have not identified a basis for limiting its production to the Pegasus program, or to any particular single operating system. The complaint alleges that "Pegasus or another remote access trojan developed by defendants" was responsible for the data breaches, and that the programs were used "on mobile devices using the Android, iOS, and Blackberry operating systems." See Dkt. 1, ¶¶ 24, 32. Accordingly, the definition of "all relevant spyware" shall not be read to include only Pegasus, or only a single operating system's program. Under Richmark, those documents are sufficiently important and specific such that compliance with discovery obligations may not be excused.

As to the timeframe of documents that must be produced, the court concludes that, at this stage of the case, the Richmark factors weigh in favor of production for "all relevant spyware" for a period of one year before the alleged attack to one year after the alleged attack; in other words, from April 29, 2018 to May 10, 2020. See Dkt. 1, ¶ 42. If, after reviewing the relevant spyware from that timeframe, plaintiffs are able to provide evidence that any attack lasted beyond that timeframe, plaintiffs may seek further discovery at that time. At the hearing, the parties discussed the possibility of stipulating to a timeframe for the production of "all relevant spyware," and may substitute their own stipulation for the timeframe set forth in this order.

As to category (2), the court rejects defendants' argument that their production should be limited to the installation layer of the alleged spyware, and instead concludes that defendants must produce information concerning the full functionality of the relevant spyware. As discussed at the hearing, the complaint contains numerous instances alleging not only that spyware was installed on users' devices, but also that information was accessed and/or extracted from those devices. See, e.g., Dkt. 1, ¶ 27 ("Pegasus could 'remotely and covertly extract valuable intelligence from virtually any mobile device,'" . . . "intercept communications sent to and from a device, including communications over iMessage, Skype, Telegram, WeChat, Facebook Messenger, Whatsapp, and others," and could be "customized for different purposes, including to intercept communications, capture screenshots, and exfiltrate browser history."); ¶ 32 ("Pegasus or another remote access trojan" was used "for the purpose of accessing data and communications on target devices."); ¶ 41 ("Defendants' malware was designed to give defendants and their customers access to information and data on the target devices, including their communications.").

Plaintiffs also pointed out at the hearing that their first cause of action under 18 U.S.C. § 1030 expressly includes as an element that the defendant "accesses a computer" and "thereby obtains information." 18 U.S.C. § 1030(a)(2).

Defendants' proposal of producing information showing the functionality of only the

installation layer of the relevant spyware would not allow plaintiffs to understand how the relevant spyware performs the functions of accessing and extracting data, and thus, the court directs defendants to provide information sufficient to show the full functionality of all relevant spyware. Under Richmark, that information is sufficiently important and specific such that compliance with discovery obligations may not be excused.

As to category (3), the court concludes that defendants need not disclose the identities of their third-party clients. Plaintiffs are indeed correct in arguing that defendants have raised the actions of those third-party clients as a defense, and plaintiffs are permitted to discover information about what actions were taken by those third parties, but plaintiffs need not discover the specific identities of the third parties in order to discover what role defendants played in any use of alleged spyware. Here, the court also notes that defendants have "offered to stipulate that Pegasus has been used by its government customers to obtain information from target devices." Dkt. 252 at 14.

As to category (4), the court concludes that defendants need not provide specific information regarding the server architecture at this time. At the hearing, the court asked plaintiffs' counsel to identify what information could be gleaned from this category of information, and plaintiffs pointed to the ability to understand the fuller picture of how the alleged spyware functioned. Based on the information presented the court, it appears that plaintiffs would be able to glean the same information from the full functionality of the alleged spyware, as discussed in category (2) above.

Thus, overall, plaintiffs' motion to compel discovery is GRANTED in part and DENIED in part.

B. Defendants' motion to compel discovery (Dkt. 240)

Defendants' motion seeks two categories of documents: (1) plaintiffs' communications with third-party witness Citizen Lab, and (2) plaintiffs' internal documents relating to their identification of the users allegedly targeted by defendants' software. As to (2), plaintiffs produced documents after the filing of this motion, and as stated at the hearing, while the parties may still have disputes about individual documents that may be

resolved through the meet-and-confer process, there is no ripe dispute for the court to resolve at this time.

As to (1), defendants argue that the Citizen Lab communications are relevant to the claims and defenses asserted in this case because "plaintiffs' central theme in this case is that Pegasus is misused by NSO's customers against 'civil society,' and plaintiffs have specifically identified Citizen Lab as having relevant information about that core allegation." Dkt. 240 at 11.

Plaintiffs argue that they "have produced all communications between plaintiffs and Citizen Lab relevant to Citizen Lab's role related to the case, which occurred entirely before the complaint was filed." Dkt. 250 at 8. To the extent that defendants seek post-complaint communications with Citizen Lab, plaintiffs argue that defendants have "fail[ed] to explain why plaintiffs' post-complaint communications with Citizen Lab are likely to have any connection to the case." Id.

The court concludes that defendants have not shown how the requested discovery is warranted under Rule 26(b)(1). Defendants argue that the "core allegation" of the complaint is that "Pegasus is misused by NSO's customers against 'civil society,'" but defendants have not explained how the "civil society" allegation relates to any of the specific three causes of action that remain operative in the case, or any of the specific affirmative defenses asserted in response. In fact, in a footnote in their reply, defendants offer that "[i]f plaintiffs would agree to withdraw from their case Citizen Lab's contention that Pegasus was used against members of 'civil society' rather than to investigate terrorism and serious crime, there would be much less need for this discovery." See Dkt. 258 at 4, n.1. It appears from that representation that the "civil society" allegation appears to be an ancillary part of this case – rather than relating to one of the elements of the asserted claims or defenses in this case. On that basis, the court fails to see the relevance of the requested discovery, and thus, denies defendants' motion to the extent that it seeks post-complaint communications between plaintiffs and Citizen Lab.

C. Defendants' motion for relief from case management schedule (Dkt. 265)

Defendants have filed a motion for relief from the case management schedule, seeking approximately a six-month extension for discovery deadlines, as well as extended deadlines for summary judgment and trial. At the hearing, the court stated that defendants' motion was granted in large part. As stated at the hearing, expert disclosures shall be due by August 30, 2024, the start of trial shall be continued to March 3, 2025, and the parties shall submit a stipulation as to the remaining dates. The parties' stipulation shall conform with this court's standing order and allow at least 120 days between the summary judgment hearing and the start of trial.

Also, as stated at the hearing, by granting defendants' motion, the additional two motions filed by plaintiffs – namely, the motion for interim schedule relief (Dkt. 279) and administrative motion to shorten time (Dkt. 280) are denied as moot.

CONCLUSION

For the foregoing reasons, plaintiffs' motion to compel discovery (Dkt. 236) is GRANTED in part and DENIED in part, defendants' motion to compel discovery (Dkt. 240) is DENIED, and defendants' motion for relief from the case management schedule (Dkt. 265) is GRANTED. Plaintiffs' motion for interim schedule relief (Dkt. 279) and administrative motion to shorten time (Dkt. 280) are denied as moot. The parties' motions to seal (Dkt. 235, 239, 249, 257, 260, 264, 272, 276) are also GRANTED.

IT IS SO ORDERED.

Dated: February 23, 2024

/s/ Phyllis J. Hamilton
PHYLLIS J. HAMILTON
United States District Judge

United States District Court
Northern District of California